

# i春秋\_真的很简单\_过程记录（坑吐了。。。）

原创

Felix\_zc 于 2019-09-19 22:15:56 发布 8608 收藏 2

分类专栏: [渗透测试](#) [writeup](#) 文章标签: [渗透测试](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_19980431/article/details/101035672](https://blog.csdn.net/qq_19980431/article/details/101035672)

版权



[渗透测试](#) 同时被 2 个专栏收录

2 篇文章 0 订阅

订阅专栏



[writeup](#)

4 篇文章 0 订阅

订阅专栏

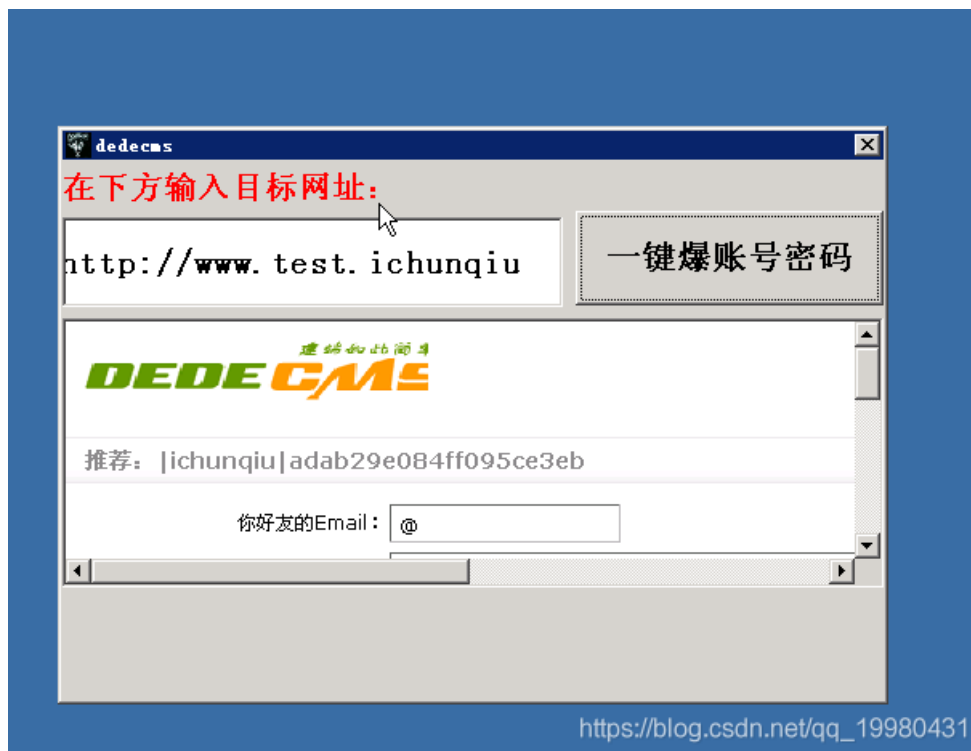
## 0x01

打开实验环境, 根据提示打开实验工具dedeCMS (坑一)

等等, 我的工具呢??? 在实验环境里提供的工具中有个dedecms5.7但是不好用啊

WTF???

实在不行去网上搜了下攻略, 发现要自己下载dedecms, 一点提示都没有, , , 好坑啊



如图, 得到网站管理员账号密码

后面的明显是md5加密后的密码, 不过数了数只有20位, 百度后得知dedecms的特点就是这样

在线破解一下得到密码: 这里推荐一下这个网站, [MD5免费在线解密](#)

## 输入让你无语的MD5

adab29e084ff095ce3eb

解密

md5

only\_system


[https://blog.csdn.net/qq\\_19980431](https://blog.csdn.net/qq_19980431)

### 0x02

查找后台地址，手动输了几个常见的，结果不行；用御剑扫了一下，结果也扫不出来

dedeCMS漏洞：mysql\_error\_trace.inc 文件里会残留后台路径。

dedeCMS目录中的data/mysql\_error\_trace.inc文件，是记录数据库出错信息。一般是用于网站存在错误，系统自动记录在该文件中，进一步说，就是该文件是记录sql错误信息的文件，类似于日志功能，关键是它会记录后台路径。



```
<?php exit();  
/*  
Page: /ichunqiu2/  
Error: 无法使用数据库  
Time2015-12-31 14:52:22  
*/  
?>  
<?php exit();  
/*  
Page:/lichunqiul/article_keywords_main.php?mima=1111  
Error: Mysql service has gone away <br />  
*/  
?>
```

[https://blog.csdn.net/qq\\_19980431](https://blog.csdn.net/qq_19980431)

发现后台地址，用刚才爆破出的密码登陆进去，（坑二）谷歌浏览器没法登录，用火狐



登陆进去之后根据手册可以用菜刀，于是乎：

利用管理员权限添加模板



## 0x03

菜刀连上之后使用虚拟终端访问桌面文件夹；

windows NT的桌面路径为C:\Documents and Settings\Administrator\桌面

切换到目标路径后修改文件权限

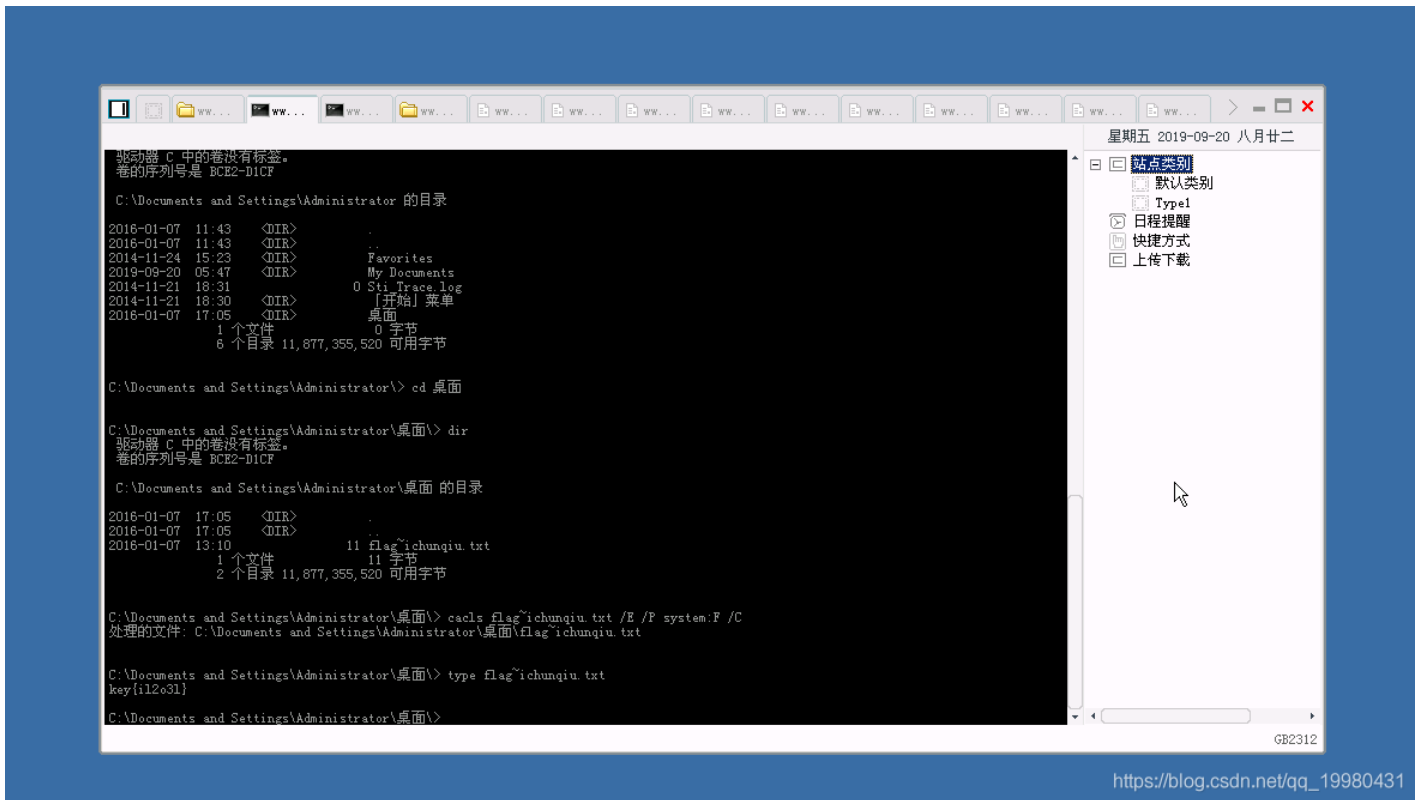
```
cacls flag~ichunqiu.txt /E /P system:F /C
```

参数说明：

/E：编辑访问控制列表而不替换；

/P user:perm 替换指定用户的访问权限（F是完全控制的意思）；

/C：在出现拒绝访问错误时继续。处理成功后，再一次查看文件访问控制权限，SYSTEM已经修改为F：完全控制，用type命令查看flag文件即可得到答案。



最后得到flag提交然后答对了1/3，嘻嘻嘻嘻

□